

Incoming ports

Product	Purpose	Ports and protocols	Configurable
FortiAP-S	Syslog, Registration, Quarantine, Log & Report	TCP/443	
	CAPWAP	UDP/5246-5247	
FortiAuthenticator	Policy Authentication through Captive Portal	TCP/1000	
	RADIUS Disconnect	TCP/1700	
FortiClient	Remote IPsec VPN	UDP/500, UDP/4500	Yes
		ESP (IP 50)	
	Remote SSL VPN	TCP/443	Yes
	Remote SSL VPN when DTLS enabled	UDP/443	Yes
	SSO Mobility Agent, FSSO	TCP/8001	
	Compliance and Security Fabric	TCP/8013	Yes
FortiExtender	Control channel	UDP/5246	Yes
	Data channel	UDP/25246	Yes
FortiGate	HA Heartbeat	ETH Layer 0x8890, 0x8891, 0x8893	
	HA Synchronization	TCP/703	
		UDP/703	
	Administrator Access	TCP/22, TCP/80, TCP/443	Yes
		ICMP	
	IPsec VPN	UDP/500, UDP/4500	Yes
		ESP (IP 50)	
	IPsec VPN Forward Error Correction	UDP/50000	
	Unicast Heartbeat for Azure	UDP/730	
	DNS for Azure	UDP/53	
	Security Fabric	UDP/8014	

Product	Purpose	Ports and protocols	Configurable
FortiGuard	IPv4 FGFM tunnel	TCP/541	
	IPv6 FGFM tunnel	TCP/542	
FortiManager	IPv4 FGFM tunnel	TCP/541	
	IPv6 FGFM tunnel	TCP/542	
FortiPortal	API for communication (FortiOS REST API)	TCP/443	
FortiToken Mobile	Approve/deny response from FortiToken Mobile	TCP/4433	Yes
FSSO server	FSSO	TCP/8001	Yes
Others	Administrator Access (SSH, HTTPS, HTTP)	TCP/22, TCP/80, TCP/443	Yes
		ICMP	
	Policy Override Authentication	TCP/443, TCP/8008, TCP/8010	
	Policy Override Keepalive	TCP/1000, TCP/1003	
	SSL VPN	TCP/443	Yes
	ACME service	TCP/80, TCP/443	
	AeroScout Vendor port	UDP/1144	
	External captive portal authentication with FortiAP in bridge mode	UDP/2000	
	RADIUS DAS feature - RFC 5176	UDP/3799	



Enabling some services will cause additional standard ports to open as the protocol necessitates. For example, enabling BGP will open TCP port 179. See [View open and in use ports](#) for more information.

Outgoing Ports

Product	Purpose	Ports and protocols	Configurable
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514	
FortiAP	CAPWAP	UDP/5246-5247	
FortiAuthenticator	LDAP, PKI Authentication	TCP/389	
		UDP/389	
	RADIUS	UDP/1812	
	FSSO	TCP/8000	
	RADIUS Accounting	UDP/1813	
	SCEP	TCP/80, TCP/443	
	CRL Download	TCP/80	
	External Captive Portal	TCP/443	
FortiExtender	Data port	UDP/5246, UDP/25246	Yes
FortiGate	HA Heartbeat	ETH Layer 0x8890, 0x8891, 0x8893	
	HA Synchronization	TCP/703	
		UDP/703	
	IPsec VPN	UDP/500, UDP/4500	Yes
		ESP (IP 50)	
	IPsec VPN Forward Error Correction	UDP/50000	
	Unicast Heartbeat for Azure	UDP/730	
FortiGate Cloud	Registration, Quarantine, Log & Report, Syslog, Contract Validation	TCP/443	
	OFTP	TCP/514	
	Management	TCP/541	

Product	Purpose	Ports and protocols	Configurable
FortiGuard	AV/IPS update	TCP/443, TCP/8890	
	Cloud Application Database	TCP/9582	
	FortiGuard Queries	UDP/53, UDP/8888	
		TCP/53, TCP/443, TCP/8888	
	DNS	UDP/53, UDP/8888	
	Registration	TCP/80	
	Alert Email, Virus sample	TCP/25	
	Management, Firmware, SMS, Licensing, Policy Override	TCP/443	
	Central Management, Analysis	TCP/541	
	IPv4 FGFM tunnel	TCP/541	
	IPv6 FGFM tunnel	TCP/542	
	Secure DNS filter	TCP/53, TCP/853	
	IPAM Service	TCP/443	
	IoT Service	TCP/443	
	FortiDDNS	TCP/443	Yes
	FortiGuard persistent connection for updates (2U and VM models only)	TCP/443	
FortiManager	IPv4 FGFM management	TCP/541	
	IPv6 FGFM management	TCP/542	
	Log & Report	TCP/514	
	AntiSpam, WebFilter queries	UDP/53, UDP/8888	
		TCP/8888	
	Registration for license validation and UTM updates (AV, IPS)	TCP/443, TCP/8890	
FortiSandbox	OFTP	TCP/514	
FortiSwitch	FortiLink	UDP/5246-5247	Yes
FortiToken Cloud	Two factor authentication request to FortiToken Cloud (ftc.fortinet.com)	TCP/8686	

Product	Purpose	Ports and protocols	Configurable
FortiToken Mobile	Two factor request to push proxy (push.fortinet.com)	TCP/443	
	Using FAC, the request is sent to FAC	UDP/1812	
FSSO	FSSO	TCP/8001	Yes
Others	email notification	TCP/465	Yes
	netflow collector	UDP/2055	Yes
	sflow collector	UDP/6343	Yes

Change Log

Date	Change Description
2022-03-31	Initial release.